

Docket No. 00-022-MIS

CLAIMS:

What is claimed is:

09593777 " 061500

Sub 2a1

1. A method for securing a transaction comprising:
receiving a request for a digest from a requestor;
retrieving a master key;
retrieving unique client information;
creating the digest by hashing the unique client
information and the master key; and
returning the digest and the unique client
information to the requestor, wherein the digest and the
unique client information will be used for transacting
with a third party.

2. The method recited in claim 1 above, wherein the
request further comprises unique requestor information
and creating the digest further comprises hashing the
unique requestor information.

3. The method recited in claim 1 above, wherein the
request includes unique merchant information which is
used to access the master key.

4. The method recited in claim 1 above, wherein the
unique client information includes a reference number,
the reference number being one of a plurality of
reference numbers provided to the client by the third
party.

5. The method recited in claim 1 above, wherein
creating the digest by hashing is performed by a smart
card.

Docket No. 00-022-MIS

1 6. The method recited in claim 1 above further
2 comprises encrypting the unique client information prior
3 to retrieving the unique client information.

1 7. The method recited in claim 1 above, wherein the
2 transaction is a credit card transaction, the third party
3 is a credit card issuer and the requestor is a merchant,
4 further wherein the requestor information includes
5 information describing at least one of a merchant
6 identifier which is specific to the credit card issuer, a
7 transaction identifier which is specific to the credit
8 card issuer and purchase information which is specific to
9 a purchase initiated by the client.

1 8. A method for securing a transaction comprising:
2 receiving, into a smart card, a data transmission
3 from a merchant, wherein the data transmission includes
4 unique merchant information, and a request for a billing
5 digest;
6 retrieving unique client information, from the smart
7 card memory;
8 retrieving a master key, the master key being known
9 to a credit card issuer;
10 creating the billing digest by hashing the unique
11 client information, the master key and the unique
12 merchant information onboard the smart card; and
13 passing the billing digest, the unique merchant
14 information and the unique client information to the
15 requestor.

09598777 "051500

Q1

Docket No. 00-022-MIS

1 9. The method recited in claim 8 above, wherein the
2 unique client information includes a reference number,
3 the reference number being one of a plurality of
4 reference numbers provided to the client by the credit
5 card issuer.

1 10. The method recited in claim 8 above further
2 comprises encrypting the unique client information and
3 the unique merchant information prior to passing the
4 information to the merchant.

1 11. A method for securing a transaction comprising:
2 sending a data transmission to a client's smart
3 card, wherein the data transmission includes unique
4 merchant information and a request for a billing digest;
5 receiving the billing digest, the unique merchant
6 information and unique client information from the
7 client's smart card, the billing digest being hashed from
8 the unique merchant information, unique client
9 information and secret information from the client's
10 smart card; and
11 transmitting the unique merchant information and
12 unique client information from the client's smart card to
13 a credit card issuer.

1 12. The method recited in claim 11 above further
2 comprises receiving a response from the credit card
3 issuer.

1 13. A method for securing a transaction comprising:

0959377 2236560

0959377 2236560

0959377 2236560

Docket No. 00-022-MIS

2 receiving a transaction request from a requestor,
3 wherein the request includes a digest and unique client
4 information;

5 accessing a master key based on the unique client
6 information;

7 creating an authorization digest by hashing the
8 unique client information and the master key;

9 comparing the authorization digest with the digest
10 from the requestor; and

11 returning a response to the requestor, the content
12 of the response being based on an outcome of the
13 comparison of the authorization digest with the digest
14 from the requestor.

1 14. The method recited in claim 13 above, wherein the
2 request includes unique requestor information and
3 creating the authorization digest further comprises
4 hashing the unique requestor information.

1 15. The method recited in claim 13 above, wherein the
2 unique client information includes a reference number,
3 the reference number being one of a plurality of
4 reference numbers provided to the client by the third
5 party.

1 16. The method recited in claim 15 above further
2 comprises:

3 accessing all previously used reference numbers
4 associated with the unique client information;

09598777 "061601

09598777 "061601

Docket No. 00-022-MIS

5 comparing the previously used reference numbers with
6 the reference number contained in the unique client
7 information; and

8 returning a response to the requestor, the content
9 of the response being based on the outcome of the
10 comparison of the previously used reference numbers with
11 the reference number contained in the unique client
12 information.

1 17. The method recited in claim 13 above, wherein
2 creating the authentication digest by hashing is
3 performed by a smart card.

5 18. The method recited in claim 13 above further
6 comprises decrypting the unique client information prior
7 accessing the master key.

1 19. The method recited in claim 13 above, wherein the
2 transaction is a credit card transaction and the
3 requestor is a merchant, further wherein the requestor
4 information includes information describing at least one
5 of a merchant identifier which is specific to the credit
6 card issuer, a transaction identifier which is specific
7 to the credit card issuer and purchase information which
8 is specific to a purchase initiated by the client.

1 20. A method for securing a transaction comprising:
2 generating a billing digest in a customer's smart
3 card, the billing digest being hashed from merchant
4 information, customer information and a master key;

095527-0001

[Handwritten signature]

Docket No. 00-022-MIS

5 creating an authentication digest by the credit card
6 issuer, wherein the authentication digest is hashed from
7 the merchant information, customer information and a
8 master key associated with the customer information;
9 comparing the authorization digest with the billing
10 digest; and
11 authorizing a transaction based on the comparison of
12 the authorization digest with the billing digest.

1 21. A method for securing a transaction comprising:
2 indexing a master key to an account identifier for
3 an account, wherein the account is between a customer and
4 a financial institution;
5 providing the master key to the financial
6 institution and a smart card controlled by the customer;
7 passing transaction data through a third party,
8 wherein the transaction data includes at least the
9 customer account identifier, third party information and
10 a billing digest which is created from the customer
11 account identifier, the third party information and the
12 master key.

1 22. A smart card for conducting secure transactions
2 comprising:
3 a input/output mechanism;
4 a processor; and
5 a memory containing:
6 financial account information;
7 a master key;
8 functional hashing algorithm;

055877-061600

Docket No. 00-022-MIS

9 an executable application, for executing on the
10 processor, for invoking the functional hashing
11 algorithm, wherein the functional hashing algorithm
12 creates a digest from the financial account
13 information and the master key and further wherein
14 the executable application transmits, via the
15 input/output mechanism, the digest and the financial
16 account information to a requestor.

0959877 "0616001
Q. 1 23. A system for conducting secure transactions
2 comprising:
3 a client smart card for creating a billing digest
4 from a resident client information, a resident master key
5 and imported merchant information;
6 a merchant system for requesting the billing digest
7 and for passing secure transaction information and the
8 billing digest to a financial institution, wherein the
9 transaction information comprises the client information,
10 and the imported merchant information; and
11 a financial institution for receiving the
12 transaction information and billing digest and for
13 authorizing a transaction by:
14 accessing a master key based on the client
15 information;
16 creating an authorization digest from the
17 master key, the client information and the merchant
18 information; and
19 comparing the authorization billing digest with
20 the billing digest.

1 24. A system for securing a transaction comprising:

9 returning means for returning the digest and the
10 unique client information to the requestor, wherein the
11 digest and the unique client information will be used for
12 transacting with a third party.

1 28. The system recited in claim 24 above, wherein the
2 creating means for creating the digest by hashing is
3 performed by a smart card.

05590777

Docket No. 00-022-MIS

1 29. The system recited in claim 24 above further
2 comprises encrypting means for encrypting the unique
3 client information prior to returning the unique client
4 information.

1 30. The system recited in claim 24 above, wherein the
2 transaction is a credit card transaction, the third party
3 is a credit card issuer and the requestor is a merchant,
4 further wherein the requestor information includes
5 information describing at least one of a merchant
6 identifier which is specific to the credit card issuer, a
7 transaction identifier which is specific to the credit
8 card issuer and transaction data which is specific to a
9 transaction initiated by the client.

1 31. The system recited in claim 24 above further
2 comprises:
3 fingerprint reading and identification means for
4 reading a fingerprint and authorizing a client based on
5 an identity of a client's fingerprint.

1 32. A system for securing a transaction comprising:
2 receiving means for receiving a transaction request
3 from a requestor, wherein the request includes a digest
4 and unique client information;
5 accessing means for accessing a master key based on
6 the unique client information;
7 creating means for creating an authorization digest
8 by hashing the unique client information and the master
9 key;

0059377-061600

Ant
A

Docket No. 00-022-MIS

10 comparing means for comparing the authorization
11 digest with the digest from the requestor; and
12 returning means for returning a response to the
13 requestor, the content of the response being based on the
14 outcome of the comparison of the authorization digest
15 with the digest from the requestor.

1 33. The system recited in claim 32 above, wherein the
2 request includes unique requestor information and
3 creating the authorization digest further comprises
4 hashing the unique requestor information.

1 34. The system recited in claim 32 above, wherein the
2 unique client information includes a reference number,
3 the reference number being one of a plurality of
4 reference numbers provided to the client by the third
5 party.

1 35. The system recited in claim 34 above further
2 comprises:

3 accessing means for accessing all previously used
4 reference numbers associated with the unique client
5 information;

6 comparing means for comparing the previously used
7 reference numbers with the reference number contained in
8 the unique client information; and

9 returning means for returning a response to the
10 requestor, the content of the response being based on the
11 outcome of the comparison of the previously used
12 reference numbers with the reference number contained in
13 the unique client information.

09598777.06#0001

Docket No. 00-022-MIS

1 36. The system recited in claim 32 above, wherein
2 creating the authentication digest by hashing is
3 performed by a smart card.

1 37. The system recited in claim 32 above further
2 comprises decrypting the unique client information prior
3 accessing the master key.

1 38. The system recited in claim 32 above, wherein the
2 transaction is a credit card transaction, the third party
3 is a credit card issuer and the requestor is a merchant,
4 further wherein the requestor information includes
5 information describing at least one of a merchant
6 identifier which is specific to the credit card issuer, a
7 transaction identifier which is specific to the credit
8 card issuer and transaction data which is specific to a
9 transaction initiated by the client.

1 39. A computer program product for securing a
2 transaction embodied on a computer readable medium
3 comprising:

4 receiving instructions for receiving a request for a
5 digest from a requestor;

6 retrieving instructions for retrieving a master key;

7 retrieving instructions for retrieving unique client
8 information;

9 creating instructions for creating the digest by
10 hashing the unique client information and the master key;
11 and

12 returning instructions for returning the digest and
13 the unique client information to the requestor, wherein

0959377 061600

Q. Conf

Docket No. 00-022-MIS

14 the digest and the unique client information will be used
15 for transacting with a third party.

1 40. A computer program product for securing a
2 transaction embodied on a computer readable medium
3 comprising:

4 receiving instructions for receiving, into a smart
5 card, a data transmission from a merchant, wherein the
6 data transmission includes unique merchant information,
7 and a request for a billing digest;

8 retrieving instructions for retrieving unique client
9 information, from the smart card memory;

10 retrieving instructions for retrieving a master key,
11 the master key being known to a credit card issuer;

12 creating instructions for creating the billing
13 digest by hashing the unique client information, the
14 master key and the unique merchant information onboard
15 the smart card; and

16 passing instructions for passing the billing digest,
17 the unique merchant information and the unique client
18 information to the requestor.

0959877-061600